Received: 29 February 2020 | Revised: 09 October 2020 | Accepted: 21 March 2021

DOI: 10.1002/asjc.2567

REGULAR PAPER

# Security-Aware Optimal Actuator Placement in Vehicle Platooning

Mohammad Hossein Basiri*[1] | Mohammad Pirani[2] | Nasser L. Azad[3] | Sebastian Fischmeister[1]

[1]Department of Electrical and Computer Engineering, University of Waterloo, ON, Canada
[2]Department of Electrical and Computer Engineering, University of Toronto, ON, Canada
[3]Department of Systems Design Engineering, University of Waterloo, ON, Canada

**Correspondence**
*Mohammad Hossein Basiri. Email: mh.basiri@uwaterloo.ca

**Abstract**

Vehicle platooning, as a large class of cyber-physical systems, is prone to be under the risk of cyber attacks. One (or more) external intelligent intruder(s) might attack one (or more) of the vehicles participating in a platoon. This paper proposes a general approach to find an optimal actuator placement strategy according to the Stackelberg game between the attacker and the defender. The game payoff is the energy needed by the attacker to steer the consensus follower-leader dynamics of the system towards his desired direction. The attacker tries to minimize this energy while the defender attempts to maximize it. Thus, based on the defined game and its optimal equilibrium point, the defender(s) selects optimal actuator placement action to face the attacker(s). Both cases of single attacker–single defender and multiple attackers–multiple defenders cases are investigated. Furthermore, we study the effects of different information flow topologies, namely the unidirectional and bidirectional data transfer structures. Besides, the impacts of increasing the connectivity among the nodes on the security level of the platoon are presented. Simulation results for $h$–nearest neighbor platoon formations along with experimental results using the scaled cars governed by Robotic Operating System (ROS) verify the effectiveness of the method.

**KEYWORDS:**
Security, game theory, actuator placement, Stackelberg attacker-defender game, vehicle platooning

## 1 | INTRODUCTION

### 1.1 | Motivation

Transportation industry is encountering various demanding requirements, which are highly critical in the last few decades. Increasing road throughput, passenger comfort, fuel consumption, safety, and security are some of the most important ones [70, 35, 58]. These challenges lead to new trends of automotive technologies such as connected vehicles; thereby, platoons have emerged. It has been extensively shown that platoons are capable of increasing the road capacity, optimizing the fuel consumption resulting in ecological driving, and enhancing the safety of the highway traffic [16]. Platoons could be formed based on different spacing policies and can be governed by different formation control techniques such as traditional linear/non-linear controllers, optimal control methods, and more advanced consensus algorithms [22, 37, 39]. Getting more developed through using more effective data communication structures, connected vehicles are equipped with different information flow topologies to facilitate and improve the efficacy of data transfers. Predecessor-follower (PF), predecessor-leader follower (PLF), two-predecessors follower (TPF), two-predecessors-leader follower (TPLF), all-predecessors follower (APF), all-predecessors-leader follower (APLF), and $h$–nearest neighbor are some of the instances [72, 46]. These structures can be exploited either in a unidirectional or a bidirectional data transmit. In this paper, we mainly focus on the $h$–nearest neighbor platoons benefiting from either unidirectional or bidirectional data communications.

The topologies mentioned earlier, physically utilize wireless communication devices such that they can exchange data, including inter-vehicular distance, speed, and acceleration. In this respect, connected cars typically take advantage of different communication environments, namely Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Cloud (V2C), Vehicle-to-Broadband (V2B), and Vehicle-to-Roadside (V2R) [19, 59]. V2V communications can provide direct data transfer with a much lower delay compared to radars [65] and enable vehicles to drive closely with short inter-vehicular distances. This will increase the amount of road throughput and reduce the need for developing more road network. In this context, Cooperative Adaptive Cruise Control (CACC) system has been widely developed featuring the possibility of coordination between connected vehicles aiming at enhancing the fuel efficiency, safety, driving comfort, and road throughput [42, 25, 38, 65, 43, 54, 55, 11].

As was mentioned before, vehicle platoons lie under a wide class of newly emerged systems, namely Cyber-Physical Systems (CPS). When CPS comes into view, control, computation, and networking bind together to form a suitable infrastructure for control and systems purposes. Having taken advantage of networking and wireless communications, CPS could develop a vast range of large scale widespread control systems. However, this might bring up a substantial challenge, which is the vulnerability of CPS against cyber attacks. Although there has been a large amount of research addressing the security of CPS, those systems still suffer from the lack of secure performance in the presence of possible malicious intruders [9]. Vehicle platoons, as a large class of CPS, incorporate the physical dynamical systems, referred to as the physical layer, with the wireless communication systems indicating the cyber layer [32]. Therefore, these systems need to guarantee a safe and secure performance in the case of dealing with unreliable and compromised networks. In recent years, researchers have been concerned about possible vulnerabilities of vehicle platoons against cyber attacks as well as communication delays [5, 18, 44, 50, 49]. Hence, one of the most prominent aspects of vehicle platooning is to ensure its security while one (or more) intruder(s) intend to devastate the performance of the platoon by injecting attack signals to one or more components of the system [12]. The injected attack signal could be of a physical one affecting the dynamical quantities of the vehicles or any deterioration of the communication framework existing among the nodes. The vulnerability of a platoon against attacks can also be caused by insecure individual vehicles participating in the platoon. Thus, securing single vehicles individually is also essential to ensure the security of the connected vehicles as a whole. In this regard, a possible means of attack on a single vehicle could be to exploit the vulnerability of one of the components of the vehicle allowing access to its CAN bus [67]. This has been the case in several real car attacks occurred recently [1]. In this paper, we let the attacker be able to inject acceleration attack signals to the longitudinal dynamics of one (or more) of the vehicles present in the platoon and try to infer the best defense strategy to mitigate the attack effects.

## 1.2 | Related Works

Over the recent years, researchers have introduced algorithms to overcome the security threats of connected vehicles with different approaches [4, 7, 8]. For instance, [47] views the problem by capturing the control-theoretic methods to address the resiliency of the connected vehicles against the adversary. Encryption of the data transmitted through the platoon, Quality of Service (QoS), and safety awareness of the vehicles are other techniques that have been exploited to address the privacy leakage of a platoon [52, 31, 51, 21]. Furthermore, safety issues that may arise due to possible malfunctioning of some redundant sensing/communication devices installed on the vehicles have been addressed in literature [56, 13]. Observer-based techniques have also been introduced to tackle the packet drop phenomenon in the network among the vehicles without compromising the overall performance [14]. Researchers have also proposed classic approaches to deal with security in cooperative vehicles, such as adaptive control, robust control, and sliding mode control [2, 33, 30, 57, 29, 71, 17, 66, 69]. Besides, game-theoretic approaches, in some instances interlaced with graph-theoretic techniques, have been shown in several paradigms to be quite fruitful to confront the security issues of control systems [10, 74, 24, 41, 36, 23]. For instance, authors in [36], employed a game-theoretic framework to confront the jamming attack threatening remote state estimation in general CPS. In [23] the minimum relative distance among two consecutive vehicles is derived based on a game-theoretical optimal control scheme. The authors have verified that this minimum safe distance heavily depends on the maximum deceleration ability of the follower vehicle. In [24], the authors study the optimal control action for a standard discrete-time linear quadratic Gaussian system in the presence of an intelligent intruder, who jams the communication link among the controller and the plant, by defining Nash/Stackelberg game problems. In [41], the evolution of the networked control system is cast as a consensus model within the cooperative games in order to apply the potential games to cooperative control problems. Those cooperative games were also investigated in terms of their resiliency against the communication failures imposed by an intruder [3, 15]. As such, vehicle platooning equipped by inter-vehicular data connectivities and formation controllers could inherently benefit from the mentioned literature to address the security challenges during attacks performed by an external adversarial attacker. To date, there is no *systematic* and *general* procedure to mitigate the intelligent attack effects imposed on a platoon with arbitrary internal communication topology and formations. In fact, the current literature suffers from the lack of a general work-around for secure platooning which is independent of the employed communication topology, number of attackers, and attack location. The authors have recently proposed Nash game solutions for sensor placement problem in vehicle platooning to detect attack effects and increase the security level of the system [10]. The current work is basically different from [10] in terms of the inherent problem, i.e., optimal actuator placement to defend and mitigate the attack effects and also the game formulation, which is the Stackleberg game. In addition, in this work the platoon model has been generalized to a higher order model to capture more realistic platoon dynamics.

It is worth mentioning that Stackelberg game formulation is more applicable to most of the security problems [40]. This is due to the fact that in most of these problems the leader (usually the defender) designs his strategy based on a possible worst case attack scenario that can be reasonably captured by the Stackelberg game. Besides, these games always admit an equilibrium point which determines the optimal strategy for the defender, hence, guarantees the existence of a solution for the defender.

## 1.3 | Contributions

In this paper, we deal with the security challenges of vehicle platoons equipped by distributed consensus controllers under the risk of cyber attacks. Explicitly, the contributions of current work are as follows,

- Considering the longitudinal dynamics of a vehicle, we formulate the attacker-defender game as a Stackelberg game problem (13) with the attacker(s) and the defender(s) as the game players. Both of the single attacker–single defender and multi attackers–multi defenders scenarios will be investigated. Furthermore, we study the impact of different information flow topologies, namely the unidirectional and bidirectional data transfer structures on the security level of the system.
- Two energy-related game pay-offs are introduced, namely the trace and the largest eigenvalue of the controllability Gramian matrix. The former has been introduced in complex dynamics networks literature [45, 61] and the latter is introduced in this work. Their interpretation together with their usefulness for our problem is described.
- A general algorithm to solve the Stackelberg game problem is given, whereby the optimal solution of the game determines the optimal actuator placement strategy for the defender. The proposed approach can be applied to platoon formations with arbitrary information flow topologies.
- Based on the values of the game-payoffs, the effect of increasing the connectivity among the vehicles of the platoon on its security level is demonstrated. This has a significant role from the defender's perspective who tries to mitigate the attack effects as much as possible.

## 1.4 | Notations and Definitions

We let $\mathcal{G}(\mathcal{V}, \mathcal{E})$ to denote an unweighted graph where $\mathcal{V}$ is the set of nodes (vertices) and $\mathcal{E}$ is the set of edges where $(v_i, v_j) \in \mathcal{E}$ if and only if there exists an edge between $v_i$ and $v_j$. We assume only unidirectional edges for the directed graphs, i.e., if there exists a directed edge from $v_i$ to $v_j$ in a directed graph, then there is no directed edge from $v_j$ to $v_i$. Assume $|\mathcal{V}| = n$. The adjacency matrix of a directed graph is $A_{n\times n}$ where $A_{ij} = 1$ if and only if there is an edge from $v_j$ to $v_i$ (the adjacency matrix is a symmetric matrix when the graph is undirected). The *neighbor* nodes of vertex $v_i \in \mathcal{V}$ in $\mathcal{G}$ are determined by the set $\mathcal{N}_i = \{v_j \in \mathcal{V} \mid (v_j, v_i) \in \mathcal{E}\}$. The in-degree of node $v_i$ (degree for undirected networks) is determined by $d_i = \Sigma_{v_j \in \mathcal{N}_i} A_{ij}$. The Laplacian matrix of a general graph $\mathcal{G}$ is defined as $L = D - A$, where $D = \text{diag}(d_1, \dots, d_n)$. In this paper, we denote a vector which has a one in the $i^{\text{th}}$ position and zero elsewhere by $\mathbf{e}_i$.

## 1.5 | Organization of the Paper

The remainder of this paper is organized as follows. Sec. 2 defines the problem statement including the longitudinal vehicle dynamics, objective of the platoon control, considered spacing policy, and the employed distributed controller. The attack model is also given in this section. Sec. 3 details the defined attacker-defender game along with the algorithm to solve for the equilibrium point of the game. Simulation results on $h$–nearest neighbor platoons are demonstrated in Sec. 4 showing the effectiveness of the method. Sec. 5 is devoted to the experimental results. The proposed method is implemented on a platform which creates a real platoon composed of the scaled cars governed by the ROS. Finally, conclusions and open avenues to continue this work are presented in Sec. 6.

## 2 | PROBLEM STATEMENT

### 2.1 | System Model

We consider a platoon consisting of $n$ follower vehicles each of which modeled with the following nonlinear dynamics model

$$\begin{cases} \dot{p}_i(t) = v_i(t), \\ \dot{v}_i(t) = \dfrac{1}{M}\left(\eta_T \dfrac{T_i(t)}{R_w} - C_A v_i^2 - Mgf_r\right), \; i = 1, 2, \ldots, n \\ \tau \dot{T}_i(t) + T_i(t) = T_{i,\mathrm{des}}(t), \end{cases} \tag{1}$$

where $p_i(t)$ and $v_i(t)$ are the position and velocity of vehicle $i$, respectively. $M$ denotes the vehicle mass, $C_A$ is the coefficient of aerodynamic drag, $f_r$ is the coefficient of rolling resistance, $g$ is the gravity constant, $T_i(t)$ is the actual driving/braking torque applied to the drivetrain, $T_{i,\mathrm{des}(t)}$ denotes the desired driving/braking torque, $R_w$ is the tire radius, $\tau$ is the inertial lag of vehicle powertrain, and $\eta_T$ is the mechanical efficiency of the driveline. It is assumed that the leader tracks a constant speed reference trajectory, i.e., $a_0(t) = 0$, $p_0 = v_0 t$ [73], where $p_0(t)$, $v_0(t)$, and $a_0(t)$ denote the position, velocity, and acceleration of the leader, respectively. The position output with relative degree three along with the following feedback linearization technique, which is widely used in literature [73, 63, 60, 68], are utilized to convert (1) to a linear one

$$T_{i,\mathrm{des}}(t) = \frac{1}{\eta_T}\left(C_A v_i(2\tau\dot{v}_i + v_i) + Mgf_r + Mu_i\right) R_w, \tag{2}$$

where $u_i$ is the control input applied to the system after feedback linearization. This results in

$$\tau \dot{a}_i(t) + a_i(t) = u_i(t) \tag{3}$$

where $a_i(t) = \dot{v}_i(t)$ is the acceleration of the $i^{\text{th}}$ vehicle. For the purpose of platoon control, the following 3rd-order state space model is yielded for the $i^{\text{th}}$ vehicle

$$\mathcal{P}: \begin{cases} \dot{p}_i(t) = v_i(t), \\ \dot{v}_i(t) = a_i(t), \\ \dot{a}_i(t) = -\dfrac{1}{\tau} a_i(t) + \dfrac{1}{\tau} u_i(t), \end{cases} \tag{4}$$

where $a_i(t) = \dot{v}_i(t)$ is the actual acceleration of the $i^{\text{th}}$ vehicle.

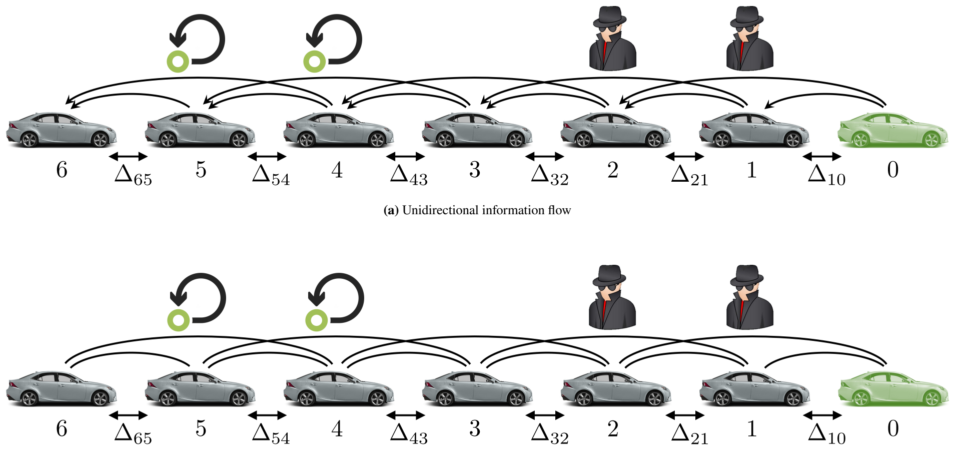
In this work, we consider a vehicle platoon wherein vehicles are connected through an $h$–nearest neighbor information flow topology (see Fig. 1). This topology has been widely utilized in automotive research community. In a directed $h$–nearest neighbor data transfer structure, each vehicle has a look-ahead data transfer communicating with its $h$ predecessors (Fig. 1a). In an undirected $h$–nearest neighbor data transfer structure, each vehicle looks ahead and back and exchanges vehicular data with its $h$ followers and predecessors (Fig. 1b).

### 2.2 | Control Objectives

The platoon control objective is for the followers to track the reference speed profile generated by the leader while maintaining a constant distance between any two consecutive vehicles, i.e.

$$\begin{cases} \lim\limits_{t\to\infty} \|v_i(t) - v_0(t)\| = 0, \\ \lim\limits_{t\to\infty} \|p_{i-1}(t) - p_i(t) - \Delta_{i-1,i}\| = 0, \end{cases} \quad i = 1, 2, \ldots, n, \tag{5}$$

where $\Delta_{i-1,i}$ is the desired constant space between consecutive vehicles $i - 1$ and $i$.



**(a)** Unidirectional information flow

**(b)** Bidirectional information flow

**FIGURE 1** 2-nearest neighbor platoons with different information flow topologies with sample attackers and actuators

The desired rigid vehicle formation will be formed by the specific constant distance $\Delta_{ij}$ between vehicles $i$ and $j$, which should satisfy $\Delta_{ij} = \Delta_{ik} + \Delta_{kj}$ for vehicles $i$, $j$, and $k$. Considering the fact that each vehicle $i$ has access to its own position, the positions, velocities and accelerations of its neighbors, and the desired inter-vehicular distances $\Delta_{ij}$, we benefit from the following consensus control law, which is a distributed CACC, and is a more advanced version of the control law introduced in [28]

$$u_i(t) = \sum_{j \in \mathcal{N}_i} k_p \left( p_j(t) - p_i(t) + \Delta_{ij} \right) + k_v \left( v_j(t) - v_i(t) \right) + k_a \left( a_j(t) - a_i(t) \right), \tag{6}$$

By collecting the states as $x_i(t) = \left[ p_i(t), v_i(t), a_i(t) \right]^\top$, and defining the tracking error vector for the $i^{\text{th}}$ vehicle, $\tilde{x}_i(t) = \left[ \tilde{p}_i(t), \tilde{v}_i(t), \tilde{a}_i(t) \right]^\top = x_i(t) - x_0(t) - \tilde{b}_i$ with $\tilde{b}_i = \left[ \Delta_{i0}, 0, 0 \right]^\top$, we get the following error dynamics model

$$\dot{\tilde{\boldsymbol{x}}}(t) = \underbrace{\begin{bmatrix} \mathbf{0}_n & I_n & \mathbf{0}_n \\ \mathbf{0}_n & \mathbf{0}_n & I_n \\ -\frac{k_p}{\tau} L_g & -\frac{k_v}{\tau} L_g & -\frac{k_a}{\tau} L_g - \frac{1}{\tau} I_n \end{bmatrix}}_{A_c} \tilde{\boldsymbol{x}}(t) \tag{7}$$

where $\tilde{\boldsymbol{x}} = [\tilde{\mathbf{P}} \quad \dot{\tilde{\mathbf{P}}} \quad \ddot{\tilde{\mathbf{P}}}]^\top = [\tilde{p}_1, \tilde{p}_2, \dots, \tilde{p}_n, \dot{\tilde{p}}_1, \dot{\tilde{p}}_2, \dots, \dot{\tilde{p}}_n, \ddot{\tilde{p}}_1, \ddot{\tilde{p}}_2, \dots, \ddot{\tilde{p}}_n]^\top$. $L_g$ is the grounded Laplacian matrix associated with the underlying graph topology of the platoon which is the reduced Laplacian matrix by removing the row and the column corresponding to the leader node. Matrix $A_c$ in (7) can also be rewritten as follows

$$A_c = A \otimes I_n - \left( E \mathcal{K}^\top \right) \otimes L_g \tag{8}$$

where $A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -\frac{1}{\tau} \end{bmatrix}$, $E = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{\tau} \end{bmatrix}$, $\mathcal{K} = [k_p \quad k_v \quad k_a]^\top$, and $\otimes$ is the Kronecker product.

## 2.3 | Attack Model

In this paper we consider a platoon under the risk of a cyber attack imposed by an intelligent intruder on one or several vehicles. It is assumed that the attacker injects an acceleration attack to the longitudinal vehicle dynamics (4). The following attacked vehicle dynamics model is used in the rest of the paper

$$\mathcal{P}_a : \begin{cases} \dot{p}_i(t) = v_i(t), \\ \dot{v}_i(t) = a_i(t) + \zeta_i(t), \\ \dot{a}_i(t) = -\dfrac{1}{\tau} a_i(t) + \dfrac{1}{\tau} u_i(t), \end{cases} \tag{9}$$

where $\zeta_i(t)$ is the injected attack acceleration signal. We assume that the leader is securely protected and can not be attacked by the intruder, hence, is able to follow the constant speed reference trajectory.

In order to mitigate the attack effects, one (or more defenders) are assumed to place self-feedback loops on one (or more) of the vehicle(s). This state-feedback controller uses the velocity of the defended vehicle(s). This technique has been introduced in literature aiming at a consensus resilient networked control system [20, 64]. Each defender will place a self-feedback loop with gain $k$ (see Fig. 1). This defense mechanism can be formulated and integrated with the distributed CACC controller (6) as follows which we refer to as CACC$_{\text{defender}}$

$$u_i(t) = \sum_{j \in \mathcal{N}_i} k_p \left( \tilde{p}_j(t) - \tilde{p}_i(t) \right) + k_v \left( \tilde{v}_j(t) - \tilde{v}_i(t) \right) + k_a \left( \tilde{a}_j(t) - \tilde{a}_i(t) \right) - k \tilde{v}_i(t), \tag{10}$$

where $k$ is the positive gain of the self-loop feedback from the velocity of the vehicle. This structure generally describes the formation control of autonomous agents [53].

Aggregating the defended CACC controller (10) with (9) in a matrix form yields the following closed-loop error dynamics

$$\dot{\tilde{\mathbf{x}}}(t) = \underbrace{\begin{bmatrix} \mathbf{0}_n & I_n & \mathbf{0}_n \\ \mathbf{0}_n & \mathbf{0}_n & I_n \\ -\frac{k_p}{\tau} L_g & -\frac{k_v}{\tau} L_g - \frac{K}{\tau} & -\frac{k_a}{\tau} L_g - \frac{1}{\tau} I_n \end{bmatrix}}_{A_a} \tilde{\mathbf{x}}(t) + \underbrace{\begin{bmatrix} \mathbf{0}_n \\ B \\ \mathbf{0}_n \end{bmatrix}}_{B_a} \boldsymbol{\zeta}(t), \tag{11}$$

where $\boldsymbol{\zeta}(t)$ is the attack vector, $K = kD_y$, $k$ is the gain of self-loop feedbacks from the speed of the vehicles, and $D_y$ is a binary diagonal matrix specifying the node(s) on which an actuator is placed through a self-feedback loop, i.e., the $i^{\text{th}}$ diagonal element of $D_y$ is 1 if the $i^{\text{th}}$ vehicle has a self-loop and is 0, otherwise. Matrix $B = [\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_f]$ specifies $f$ node(s) selected by the attacker. Note that matrix $A_a$ in (11) can also be rewritten as follows

$$A_a = A \otimes I_n - \left( E \mathcal{K}^{\top} \right) \otimes L_g - \left( E \mathbf{e}_2^{\top} \right) \otimes K \tag{12}$$

## 3 | ATTACK EFFECTS MITIGATION VIA OPTIMAL ACTUATOR PLACEMENT

In this section, we first formulate the problem as an attacker-defender game and describe its components in detail. The game-payoff, the players, and the decision variables of each of the players is explained. Then, some basics of the method, along with the details of the proposed approach, will be presented.

### 3.1 | Attacker–Defender Game

To study the confrontation of the attacker and the defender in a platoon, we formulate the problem as a game with the attacker and the defender as its players. The conflicting decision between the players arises by optimizing a game pay-off in opposite directions. We will focus on two well-known metrics describing the energy needed by the attacker to deviate the dynamics of the followers towards a direction in the state space. The game pay-offs will be explained in the next subsection. The decision variable of the attacker is the $B$ matrix, and the defender's decision variable is the diagonal matrix $K$ in (11). In fact, the attacker chooses the $B$ matrix to determine the vehicle(s) to attack attempting to minimize the energy needed to steer the consensus dynamics in the state space. On the other hand, the defender makes a decision about the $K$ matrix to equip certain vehicle(s) with the self-loops to defend making the energy required by the attacker as large as possible. The attacker-defender game is cast into a Stackelberg game formulation with the defender acting as the game leader. This formulation leads to study the optimal actuator placement for the defender based on the optimal equilibrium strategy of the defined game. More rigorously, the equilibrium point of the Stackelberg game determines the optimal decision for the defender by which he determines which vehicle(s) to place the actuator(s) on. Through this placement, the attack energy needed by the attacker to steer the system into his desired direction will be maximized; hence, the attack effects will be mitigated. Throughout the paper, it is assumed that the defender has as many actuators available as the number of attackers. The results can be simply generalized to more general cases. We formally introduce the following game

Attacker–Defender Game

The attacker injects the attack signal $\zeta_i(t)$ to $f$ vehicles to minimize his required energy (defined by one of its physical interpretations) to steer the consensus dynamics of the system towards his desired direction in the state space, while the defender places his actuators on $f$ vehicles to maximize the energy needed by the attacker. Hence, this zero-sum game is represented by either of the two following game pay-offs

$$J(B,K) = \lambda_{\max}\left(W_c(B,K)\right), \tag{13a}$$

$$J(B,K) = \mathbf{tr}\left(W_c(B,K)\right), \tag{13b}$$

where the attacker's decision is matrix $B$ to maximize $J(B,K)$ and the defender's decision determines matrix $K$ to minimize $J(B,K)$ since the game pay-offs are inversely related to the average amount of energy.

*Remark 1.* It is common in the literature that the defender knows an upper bound of the attacked nodes [62]. Here, we assume that $f$ is an upper bound of the attacked nodes, and hence, the defender acts based on this worst-case scenario. □

The game pay-offs used in (13) are defined in the following subsection.

## 3.2 | Game Pay-off Definition and Interpretation for the Actuator Placement Problem

There have been various metrics introduced in literature with different physical interpretations related to system controllability for complex dynamical networks [61, 45]. Having performed an attack on a real system, the attacker usually needs to take an energy limit action. Hence, controllability metrics dealing with the amount of input energy required to impose the attack are of our interest. Thus, we focus on two of these energy-related metrics which are widely used to quantify the controllability level of a network, namely the largest eigenvalue of the *controllabilty Gramian* matrix, and its trace. It is notable that, due to the special control input of our system, which is the attack signal, we utilize the largest eigenvalue of the controllability Gramian matrix instead of the smallest one, which is proposed in classical control literature [61, 45]. This will be explained in more detail subsequently.

### 3.2.1 | Largest Eigenvalue of the Controllability Gramian Matrix ($\lambda_{\max}(W_c)$)

The maximum eigenvalue of $W_c$ is a worst-case metric inversely related to the amount of energy required to move the system in a direction in the state space that is the easiest to control. The eigenvector corresponding to the maximum eigenvalue of $W_c$ is the direction in the state space that is the easiest to move the system. We intend to minimize $\lambda_{\max}(W_c)$ to maximize the control effort needed by the attacker so that he needs much energy to move the system in the easiest direction he has in hand.

*Remark 2.* Since the control input of our system is the attack signal (undesired input), we benefit from the largest eigenvalue of $W_c$. As this eigenvalue and its associated eigenvector pertain to the easiest direction in the state space to which the attacker can deviate the system, we target minimizing this quantity in order to make the effort needed by the attacker as large as possible. In other words, our goal is to make the system as less controllable as possible for the easiest direction the attacker has in hand. Note that in typical systems, the control input is the desired signal which imposes using the smallest eigenvalue of $W_c$ to measure the controllability of the system from the perspective of that particular input [61, 45]. □

### 3.2.2 | Trace of the Controllability Gramian Matrix ($\mathbf{tr}(W_c)$)

Trace of the controllability Gramian matrix is inversely related to the average amount of the energy required by the attacker to move the system around in the state space. We intend to minimize $\mathbf{tr}(W_c)$ to maximize the control effort needed by the attacker.

*Remark 3.* Minimization of the trace of the controllability Gramian matrix might lead to an uncontrollable system, such that $W_c \nsucc 0$, [45]. In this case, the defender's action is to maximize the energy required by the attacker to steer the system in the controllable subspace, i.e., range($W_c$). □

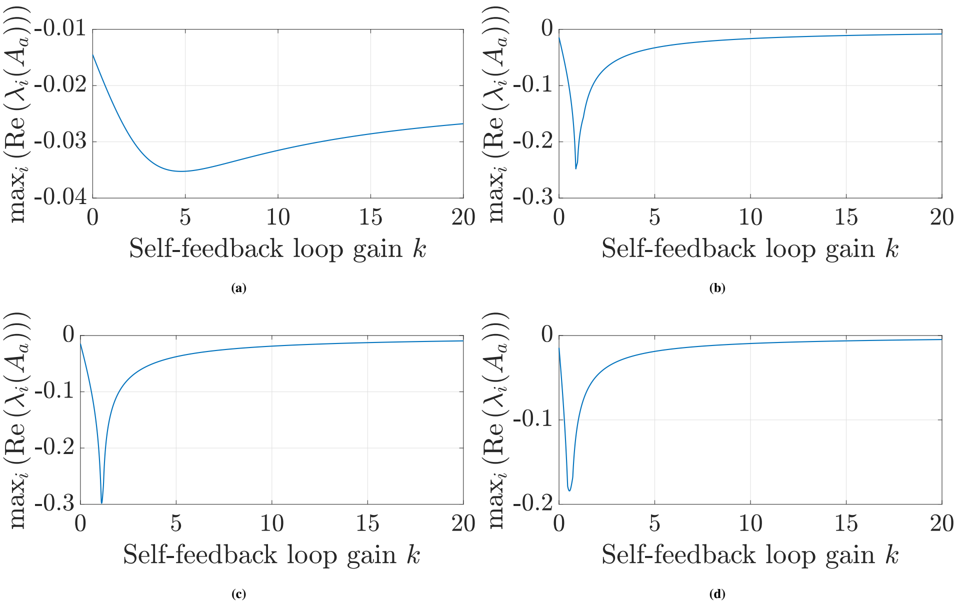


**FIGURE 2** Closed-loop stability of platoon dynamics with different actuator placement and different self-loop gains (a): Actuator placed on vehicle 1, (b): Actuator placed on vehicle 6, (c): Actuators placed on vehicles 2 and 4, (d): Actuators placed on vehicles 5 and 6

## 3.3 | Stackelberg Game Formulation

Before delving into the game formulation, we need to highlight the reason of working with Stackelberg game. It is due to the nature of our problem (which is a design problem), and we are interested in designing the optimal actuator placement in an offline fashion. In this setup, the Stackelberg game suits better. In other words, the design problem is generally considered as a passive problem which can be reasonably captured by a Stackelberg game (the reader is referred to [40] specially Table II therein for more details). Besides, in most of the security problems, owing to the existence of the leader and follower (where one of the players has the ability to enforce his strategy on the other), it is turned out that the Stackelberg game is more suitable to formulate the problem.

Considering either of the two aforementioned metrics as our game pay-off, denoted by $g(\cdot)$, the leader of the game which is the defender, solves the following optimization problem

$$J^*(K) = \min_K g(B^*(K)), \tag{14}$$

where $J^*$ denotes the optimal value of $J$. In (14), $B^*(K)$ is the attacker's best response to the defender's strategy $K$. In fact, $B^*(K)$ is the solution to the following optimization problem

$$B^*(K) = \arg\max_B g(B). \tag{15}$$

Hence, the equilibrium strategy of the Stackelberg game leading to the defender's optimal strategy is given by

$$K^* = \arg\min_K J^*(K). \tag{16}$$

Algorithm 1 summarizes the procedure for the general case of multi attackers and multi defenders to find the solution of the Stackelberg game problem. Notably, the Stackelberg game problem might have non-unique solutions; however, the game-payoff is the same for all the solutions.

Referring back to our main objective, i.e., aiming at minimizing the aforementioned controllability metrics, we first need to calculate the controllability Gramian matrix associated with the attacked and defended closed-loop dynamics (11). The symmetric positive semidefinite controllability Gramian matrix associated with dynamics model (11) is given by

$$W_c(t) = \int_0^t e^{A_a s} B_a B_a^\top e^{A_a^\top s} ds, \tag{17}$$

**Algorithm 1** STACKELBERG ATTACKER–DEFENDER GAME IN VEHICLE PLATOONING

```
Input:
Data transfer structure ($L_g$), $g(\cdot)$, $n$, number of attacker(s) ($f$)
for $i = 1 : \binom{n}{f}$ do                              ▷ $i$ is the defender index
    for $j = 1 : \binom{n}{f}$ do                          ▷ $j$ is the attacker index
        $J(B(K_i)) = g(B_j)$
    end for
    $B^*(K_i) = \arg\max_{B_j} g(B_j)$
    $J(K_i) = g(B^*(K_i))$
end for
$J^*(K) = \min_{K_i} g(B^*(K_i))$
$K^* = \arg\min_K J^*(K)$
$B^* = \arg\max_B J(K^*)$
Output:
$K^*$                ▷ Solution of the Stackelberg game problem (defender's optimal strategy)
$B^*$                ▷ Solution of the Stackelberg game problem (attacker's optimal strategy)
$J(B^*, K^*)$        ▷ Optimal game pay-off
```

which quantifies an energy-related measurement of the controllability level of the system. Eigenvectors of $W_c$ corresponding to small eigenvalues determine directions in the state space that are less controllable (require large input energy to reach), and eigenvectors of $W_c$ corresponding to large eigenvalues reflect directions in the state space that are more controllable (require small input energy to reach).

In case of an internally stable system, the state transition matrix $e^{A_a s}$ decays exponentially leading to the following finite positive definite controllability Gramian matrix

$$W_c = \int_0^\infty e^{A_a s} B_a B_a^\top e^{A_a^\top s} ds, \tag{18}$$

This infinite-horizon controllability Gramian matrix can also be computed by solving for the unique positive definite solution of the following Lyapunov equation

$$A_a W_c + W_c A_a^\top + B_a B_a^\top = \mathbf{0}. \tag{19}$$

Equation (19) forms a system of linear equations that can be easily solved. Dedicated algorithms have been proposed to solve for the solution of (19) effectively for even large scale systems [6, 26, 34]. In this paper, we exploit the second method to find the infinite-horizon $W_c$ in the interest of ease of computation. It is worth keeping in mind that since the closed-loop matrix $A_a$ incorporates the unknown defender decision variable, $K$, derivation of a closed-form of $W_c$ as a function of $K$ is burdensome. Besides, we intend to focus on the optimal strategy of the defender for different information flow topologies rather than a general solution for $W_c$. Hence, we solve (19) for $W_c$ numerically based on which we state the optimal defender strategy to mitigate the attack effects in different scenarios. It is noteworthy that our game formulation approach can be applied to increase the security level of platoons with an arbitrary number of followers equipped with different information flow topologies. Furthermore, other metrics could be exploited while applying our method for different assessments of the security-related aspects of a platoon.

*Remark 4.* Regarding the required information to form the controllability Gramian matrix, we point out that one needs to know matrices $A_a$ and $B_a$, which consist of the underlying platoon topology information. This information includes the controller gains ($k_p$, $k_v$, and $k_a$), the data transfer structure ($L_g$), and the attacker and the defender decisions determined by $B$ and $K$ matrices, respectively, which differs from those required by the consensus control law, i.e., the tracking error vector $\tilde{\boldsymbol{x}}(t)$. □

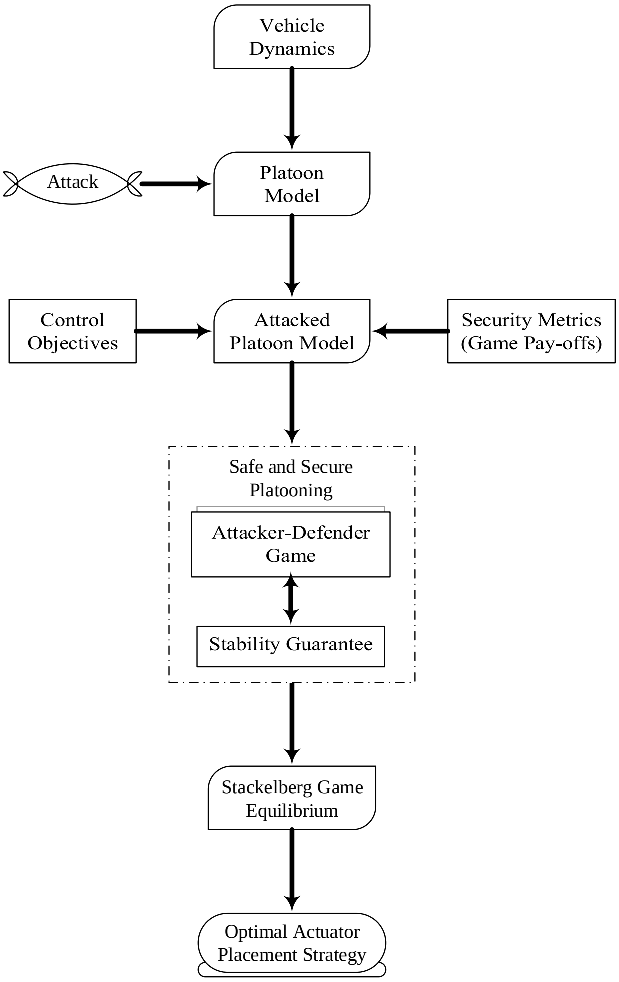

Vehicle Dynamics
Attack
Platoon Model
Control Objectives
Attacked Platoon Model
Security Metrics (Game Pay-offs)
Safe and Secure Platooning
Attacker-Defender Game
Stability Guarantee
Stackelberg Game Equilibrium
Optimal Actuator Placement Strategy

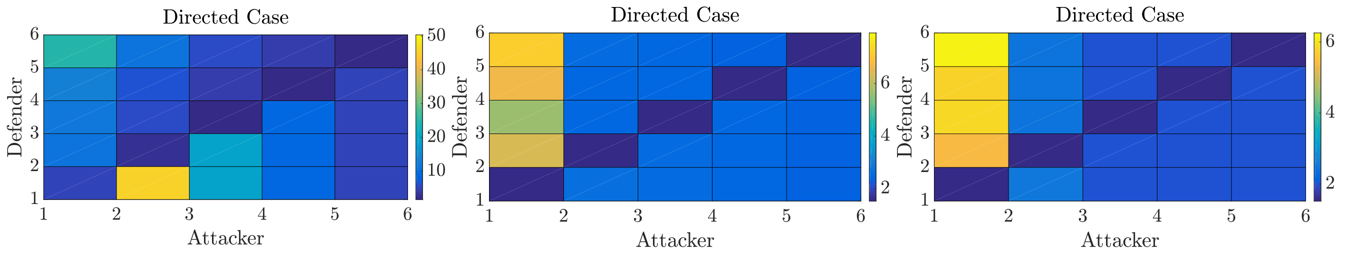
**FIGURE 3** Proposed procedure to obtain the optimal strategy for the defender

## 3.4 | Stability of the Closed-loop Platoon Dynamics

Generally, as a standard requirement, the stability of the closed-loop platoon dynamics needs to be ensured while performing the attack mitigation process. This requirement has to be met to have the desired rigid formation during our defined game. Basically, in platoon control, there are two different main stability notions defined for the closed-loop platoon dynamics, namely the *internal stability* and the *string stability*. A platoon with linear time-invariant dynamics is internally stable if and only if the least stable eigenvalue of the closed-loop system lies on the open left half-hand side of the complex plane [27]. For a platoon to be string stable, any disturbance introduced in the downstream of the platoon needs to be dampened while it is propagated along the upstream vehicles [63, 48]. In this paper, we focus on the former and leave the latter for future work. Here, to have the vehicle platoon asymptotically stable prior to any attacks occur, we benefit from a result given in [72] to choose a set of controller gains to guarantee the asymptotically stability of the platoon under study as follows

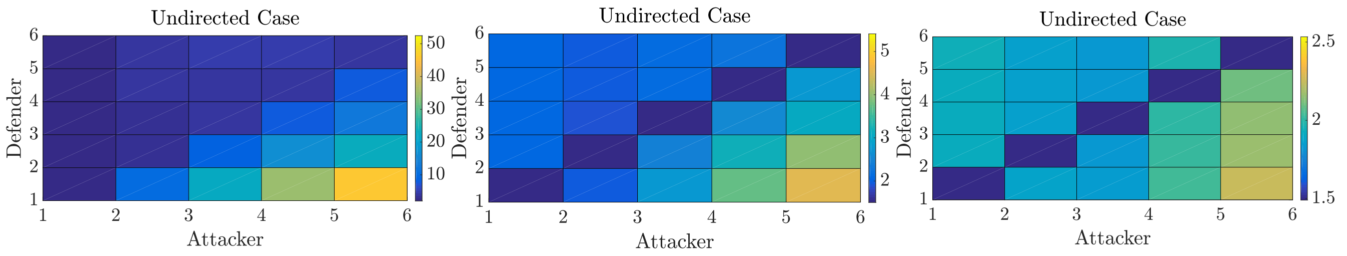
$$\begin{cases} k_p > 0, \\ k_v > \dfrac{k_p \tau}{\min_{i\in\{1,2,\dots,n\}}(\lambda_i k_a + 1)}, \\ k_a > -\dfrac{1}{\max_{i\in\{1,2,\dots,n\}} \lambda_i}. \end{cases} \tag{20}$$

where $\lambda_i$ is the eigenvalue of the grounded Laplacian matrix. Since we intend to focus on the optimal defender's strategy to mitigate the attack effects the most and the tuning of controller gains is not our concern, we simply choose $k_p = k_v = k_a = 1$,



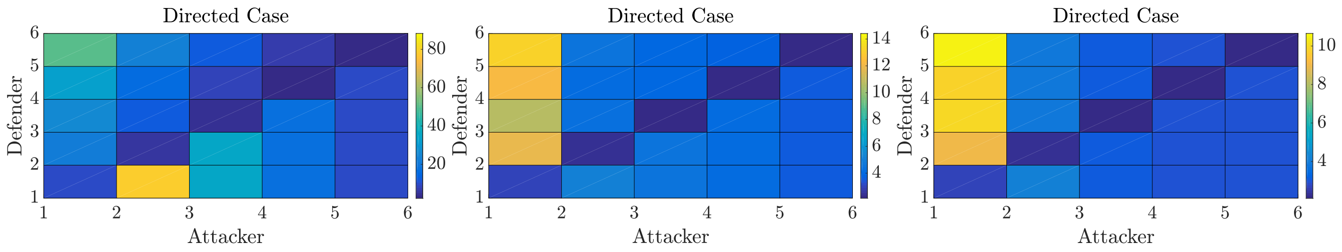
**(a)** 1-nearest neighbor **(b)** 2-nearest neighbor **(c)** 3-nearest neighbor

**FIGURE 4** Game pay-off for the attacked directed platoon with 6 followers and single attacker–single defender (game pay-off: $\lambda_{\max}(W_c)$)



**(a)** 1-nearest neighbor **(b)** 2-nearest neighbor **(c)** 3-nearest neighbor

**FIGURE 5** Game pay-off for the attacked undirected platoon with 6 followers and single attacker–single defender (game pay-off: $\lambda_{\max}(W_c)$)



**(a)** 1-nearest neighbor **(b)** 2-nearest neighbor **(c)** 3-nearest neighbor

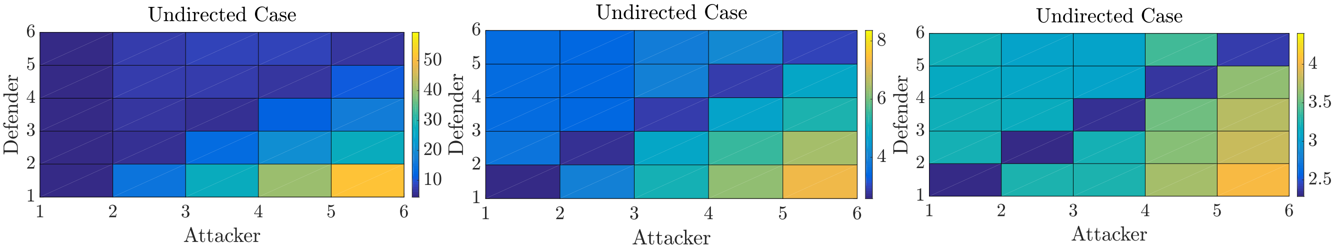
**FIGURE 6** Game pay-off for the attacked directed platoon with 6 followers and single attacker–single defender (game pay-off: $\mathbf{tr}(W_c)$)

and $k = 2$ to satisfy the mentioned conditions and focus on the optimal defender's strategy for an asymptotically stable vehicle platoon. The value for the inertial lag is chosen as $\tau = 0.5$ sec throughout the following simulations. It is known that the inertial lag is bounded, i.e., $\tau \in [0, \tau_{\max}]$, where $\tau = 0$ corresponds to the ideal case of immediate actuation. Here, we choose a typical value reported in the literature [72]. Fig. 2 shows the stability margin of the closed-loop system with the aforementioned values for $k_p$, $k_v$, and $k_a$ for some different actuator placements with different gain values. It is obvious that in all of the scenarios, including the one we chose for our subsequent simulations ($k = 2$), the platoon is asymptotically stable. It turns out that the results hold for any set of controller gains as long as the platoon remains asymptotically stable.

Fig. 3 shows the entire procedure to determine the optimal strategy for the defender.

## 4 | SIMULATION RESULTS

In this section, we present the simulation results stating the optimal actuator placement of the defender for a platoon with single attacker–single defender and multi attackers–multi defenders. Defender's optimal decision is determined based on the solution

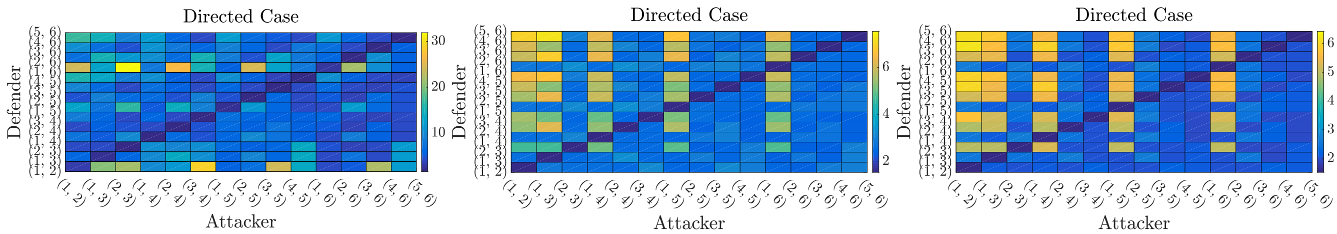


**(a)** 1-nearest neighbor

**(b)** 2-nearest neighbor

**(c)** 3-nearest neighbor

**FIGURE 7** Game pay-off for the attacked undirected platoon with 6 followers and single attacker–single defender (game pay-off: $\mathbf{tr}(W_c)$)

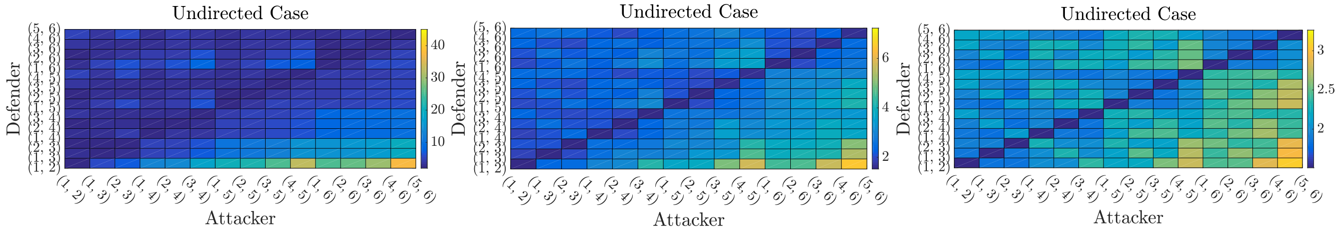


**(a)** 1-nearest neighbor

**(b)** 2-nearest neighbor

**(c)** 3-nearest neighbor

**FIGURE 8** Game pay-off for the attacked directed platoon with 6 followers and two attackers–two defenders (game pay-off: $\lambda_{\max}(W_c)$)

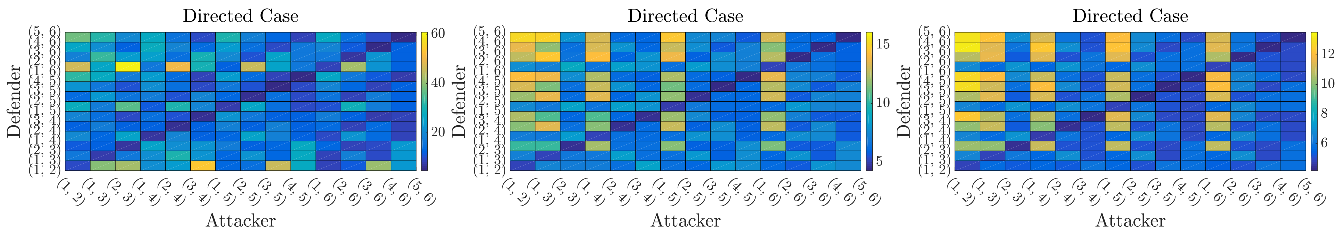


**(a)** 1-nearest neighbor

**(b)** 2-nearest neighbor

**(c)** 3-nearest neighbor

**FIGURE 9** Game pay-off for the attacked undirected platoon with 6 followers and two attackers–two defenders (game pay-off: $\lambda_{\max}(W_c)$)



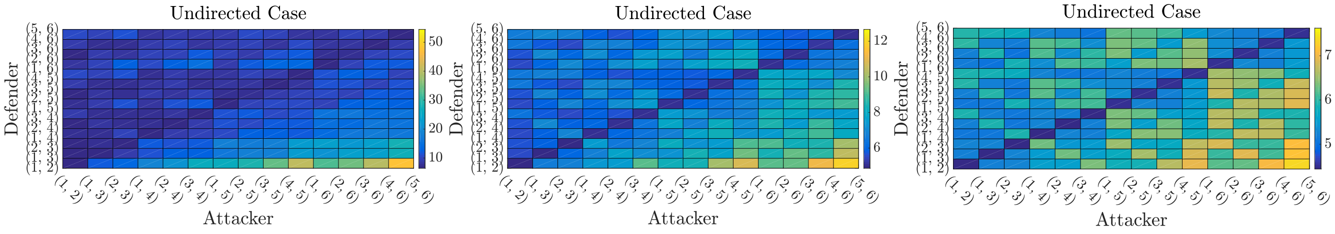
**(a)** 1-nearest neighbor

**(b)** 2-nearest neighbor

**(c)** 3-nearest neighbor

**FIGURE 10** Game pay-off for the attacked directed platoon with 6 followers and two attackers–two defenders (game pay-off: $\mathbf{tr}(W_c)$)

of the aforementioned Stackelberg game with the attacker(s) and the defender(s) as its players. Throughout the simulations, we consider a vehicle platoon consisting of 6 followers connected through the $h$–nearest neighbor information flow topology shown in Fig. 1.



**(a)** 1-nearest neighbor

**(b)** 2-nearest neighbor

**(c)** 3-nearest neighbor

**FIGURE 11** Game pay-off for the attacked undirected platoon with 6 followers and two attackers–two defenders (game pay-off: $\mathbf{tr}(W_c)$)

## 4.1 | Single Attacker–Single Defender Platoon

Let us consider a vehicle platoon under cyber attack in which the vehicles can communicate with each other through unidirectional data transfer structure. We assume that each time one of the followers is attacked and for that particular case, the defender places his actuator on each of the followers. Fig. 4 and 6 illustrate the game pay-offs for all possible combinations of the attacker-defender for two different game pay-offs. One can easily see that increasing the connectivity among the vehicles cause the game values to be decreased. This, inherently, is a desired effect from the defender's perspective. As shown in these figures, both of the controllability metrics verify this result. Another significant point which needs to be highlighted is the fact that attacking the leader's neighbor in the unidirectional data transfer structure has the worst effect the attacker can impose on the platoon. In essence, the leader's neighbor is the vehicle receiving the most original version (with the least manipulations) of the reference profile generated by the leader. Basically, when vehicle 1 is attacked, it gets harder for the rest of the followers to receive the correct form of the reference profile. This is due to the critical role of the leader's neighbor who receives the intact reference profile from the leader and broadcasts to *all* of the followers regardless of the exploited information flow topology. This is the main reason that, for example, attacking vehicle 2 in a 2-nearest neighbor (or vehicle 3 in a 3-nearest neighbor) topology will not deteriorate the security level of the platoon as much as that of when attacking the leader's neighbor.

In the bidirectional information flow scenario, a similar attacked platoon is considered except the vehicles are able to send data over a bidirectional data transfer structure. Fig. 5 and 7 show the game pay-offs for this scenario. Note that a similar result regarding the benefit of increasing the connectivity of the platoon clearly holds for the bidirectional data transfer framework.

## 4.2 | Multi Attackers–Multi Defenders Platoon

In this part, we assume the platoon is under cyber attacks imposed by more than one attacker. To avoid crowded figures in the simulations, we assume $f = 2$ and perform our analyses for both the unidirectional and bidirectional data transfer structures.

The same unidirectional and bidirectional platoons are considered except with two attackers and two defenders. The attackers might attack any pair of the vehicles and based on the defender's strategy, the value of the game pay-off is calculated. Fig. 8 and 10 show the corresponding game values. As can be seen from these figures, a more densely connected platoon makes the energy needed by the attacker larger, hence, better from the defender's perspective. In this scenario, similar to the single attacker–single defender one, the attacker can effectively endanger the security of the platoon the most by including the leader's neighbor in his attacked vehicles.

From Fig. 9 and 11, it is again verified that as the connectivity among the vehicles is increased the attacker needs to exert more energy to perform the attack. Hence, the mentioned result holds regardless of the communication environment exploited in the platoon.

*Remark 5.* In all of the presented simulations, one can clearly see that, for any combination of the attacker(s) and the defender(s), the minimum game pay-off corresponds to the case where the defender exactly places its actuator(s) on the attacked node(s). Although this precise prediction may be unrealistic, it reflects the ideal decision that could be made by the defender. Furthermore, as the actuator(s) placement gets farther from the attacked nodes, the game pay-off increases, i.e., the attacker(s) needs to spend less energy to deviate the system towards his intended direction. □

Table 1 demonstrates the optimal defender's strategy for different information flow topologies, different game pay-offs, and different number of players for the considered platoon. The numbers represent the vehicle(s) on which the defender has to place

**TABLE 1** Solution to the attacker-defender Stackelberg game (defender's optimal strategy) for the attacked platoons shown in Fig. 1

| | $f = 1$ | | | |
|---|---|---|---|---|
| | **Directed** | | **Undirected** | |
| | $\lambda_{\max}(W_c)$ | $\mathbf{tr}(W_c)$ | $\lambda_{\max}(W_c)$ | $\mathbf{tr}(W_c)$ |
| 1-nearest neighbor | 3 | 3 | 6 | 6 |
| 2-nearest neighbor | 1 | 1 | 6 | 6 |
| 3-nearest neighbor | 1 | 1 | 6 | 6 |
| 4-nearest neighbor | 1 | 1 | 6 | 6 |

| | $f = 2$ | | | |
|---|---|---|---|---|
| | **Directed** | | **Undirected** | |
| | $\lambda_{\max}(W_c)$ | $\mathbf{tr}(W_c)$ | $\lambda_{\max}(W_c)$ | $\mathbf{tr}(W_c)$ |
| 1-nearest neighbor | (2, 4) | (2, 4) | (3, 6) | (3, 6) |
| 2-nearest neighbor | (1, 4) | (1, 4) | (5, 6) | (5, 6) |
| 3-nearest neighbor | (1, 2) | (1, 2) | (5, 6) | (5, 6) |
| 4-nearest neighbor | (1, 2) | (1, 2) | (5, 6) | (5, 6) |

†The numbers represent the vehicle(s) on which the defender has to place his actuator(s).

his actuator(s). Inspired by this table, in a unidirectional vehicle platoon, it is more beneficial to place the actuator(s) at the downstream of the platoon. On the other hand, in a bidirectional vehicle platoon, placing the actuator(s) at the upstream of the platoon mitigates the attack effects more effectively. Similar results can be generated via the general method introduced in this paper for any asymptotically stable platoon equipped with self-feedback loops.

*Remark 6.* Various energy-related controllability metrics might result in different control actions. In essence, in some instances, optimizing the trace of the controllability Gramian matrix can lead to a poor controllability performance in regard to the worst-case energy needed to reach a particular state; however, it is known that the selection of optimal nodes based on this metric benefits a closed-form solution as reported in the literature [45]. In such cases, if the analyses are performed by employing a numerical perspective without concerning about a closed-form solution, the largest eigenvalue of the controllability matrix is more suitable to be used as the game pay-off to ensure an appropriate controllability index of the system. □

*Remark 7.* It is remarkable that the simulation results show off-line game pay-offs for different combinations of the players. In fact, they are not the "final optimal" solution of the Stackelberg game problem which determines the optimal decisions that need to be made by the players. For instance, as was explained earlier, the game pay-offs demonstrate that (in a unidirectional topology) the attacker can endanger the security level of the platoon the most by targeting the leader's neighbor. This is exactly what the defender (as the game leader) figures out by solving the Stackelberg game problem to design his strategy. Hence, the defender eventually takes the optimal action accordingly to face this upcoming worst-case attack imposed by the intruder. □

# 5 | EXPERIMENTAL RESULTS

## 5.1 | Basic Setup Architecture

As another verification approach to our results, we perform some experiments on a real platoon consisting of four scaled cars driving on a treadmill shown in Fig. 12. The positions, linear/angular velocities, steering, commanded throttle, actual throttle, and the State-of-Charge (SOC) of the batteries of each of the cars are exchanged between the host PC running the ROS and the vehicles through an IEEE 802.15.4-based 2.4GHz ZigBee wireless network protocol. Each of the cars is powered up by two identical batteries with the same initial SOC. The goal positions of the vehicles are commanded by the host PC, and the actual positions are captured via a central infrared camera detecting the specific Apriltags mounted on the vehicles. The vehicles find the position of their preceding car via the central camera and the PC (as the intermediate hardware) modeling the directed data

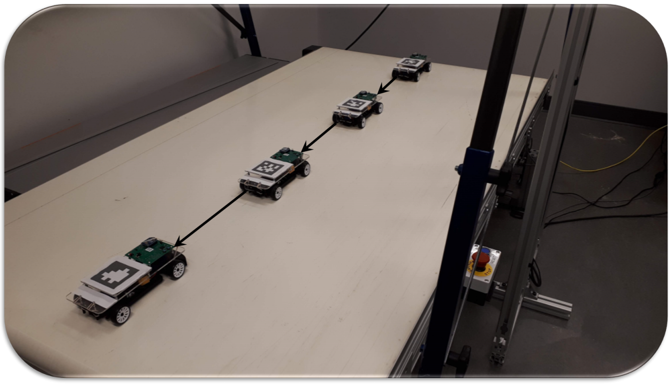


**FIGURE 12** General schematic of the experimental platoon

transfer topology. Due to the limited length of the treadmill and to have the longest possible platoon, it is formed such that the four follower vehicles track a desired speed profile generated by the host PC which is considered as a virtual leader.

## 5.2 | Attack Mitigation Experiments

In our experiments, we consider the single attacker–single defender case. Following Algorithm 1 for a 1-nearest neighbor platoon composed of four homogeneous scaled cars with a directed data transfer structure and considering the largest eigenvalue of the controllability Gramian matrix as the game pay-off, it turns out that the optimal defender strategy is to place the self-loop on the second vehicle to mitigate the worst-case attack impact caused by attacking the third vehicle of the platoon. The controllability Gramian matrix highlighting the element which reflects the optimal decision made by the players is given by

$$\lambda_{\max}(W_c) = \begin{bmatrix} 1.5678 & 9.1645 & 5.2552 & 3.6413 \\ 4.3001 & 1.5605 & 5.2552 & 3.6413 \\ 6.0162 & 4.0937 & 1.5561 & 3.6413 \\ 10.0278 & 5.6221 & 3.8836 & 1.5504 \end{bmatrix} \tag{21}$$

Four separate experiments were conducted, each of which handled an acceleration attack on one of the individual cars along with implementing the defense mechanism on the second vehicle. In other words, in experiment $i$, the vehicle $i$ is attacked, and the second vehicle defends. To reflect the amount of energy needed by the attacker to disrupt the desired rigid formation of the platoon, we consider the total dropped level of SOC of batteries of the attacked car.

Each experiment lasts for 10 minutes, wherein the first 2 minutes, we let the platoon simply run and reach its steady formation without any occurrence of attack or defense action. Having got a clear insight into the amount of dropped SOC values during our tests, we assume the attacker is able to impose his attacks with a periodic timing manner. This inherently models a severe attack scenario. It is worth keeping in mind that an intelligent attacker might not perform such a repetitive action in order not to get detected; however, in this study, we focus on the energy-related criterion of an attack rather than the attack detection. Hence, it is more appropriate for us to model such an intense attacker to have a clear view of the amount of energy he may need. The first attack occurs at $t = 2$ min., by injecting a sharp spike to the longitudinal position of the attacked car. The very first attack has a magnitude of 0.75 meters while the subsequent ones occur at every 2 seconds with a magnitude of 0.5 meters. The defense mechanism executed by vehicle 2 also has a periodic fashion. Particularly, it begins at time $t = 2$ min., lasting for 0.5 seconds with 3 seconds cooldown period between each defense. The total SOC values of the cars are sampled every 5 seconds and sent to the host PC via the XBee module. Fig. 13 shows the SOC values of the attacked car in each of the four experiments. As one can easily see from this figure, before the attack/defense onset, the SOCs decrease with a relatively low slope. Once the first attack occurs along with the defense of the second vehicle, the SOCs drop significantly. Thereafter, the SOCs decrease with relatively high slopes over the time course compared to the beginning of the experiments. As was expected, choosing the optimal solution of the Stackelberg game problem (in this case, the third vehicle), the intelligent attacker consumes the least amount of energy. Furthermore, based on the SOC values of the experiments, it is obvious that the intruder is never inclined to deviate his decision

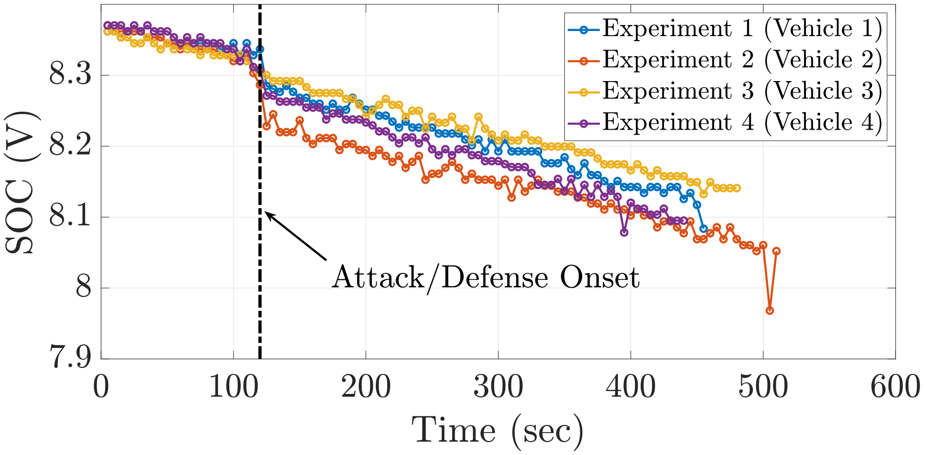


**FIGURE 13** SOC values of the attacked car in each of the four experiments

from this equilibrium point. It is also notable that experiment 2 verifies a trivial case. Rigorously, placement of both the actuator and the attack on the same node results in the most energy needed by the intruder (most dropped SOC value). However, this case is unlikely to happen in the real world. Let us consider the case in which the defender is the game leader (which is our focus in this work). In this case, the defender places its actuator on a specific node, followed by the attacker's decision. As the attacker is assumed to be aware of the defender's decision, he never attacks the defended node. On the other hand, let us consider the case where the attacker is the game leader. In this case, the intruder imposes his attack on a specific node, followed by the defender's decision. Thus, the defender definitely defends the exact same node attacked by the intruder resulting in maximizing the energy required by the attacker; however, in the real world the attacker's decision is not known beforehand.

## 6 | CONCLUSION AND FUTURE WORKS

In this paper, a game-theoretic approach has been proposed to tackle the security challenges of vehicle platoons. From the viewpoint of secure platoon control, we studied the problem of threatening a vehicle platoon by one (or more) attacker(s) who tries to deteriorate the platoon control by injection of acceleration attack signal(s) to the longitudinal dynamics of one (or more) of the vehicles. In essence, we focused on the energy needed by the attacker, as our game-payoff, to steer the consensus dynamics of the system towards his desired direction in the state space. In this regard, the attacker(s) basically tries to minimize the amount of energy needed to deviate the system dynamics, while the defender(s) faces this action by attempting to maximize that energy. This confrontation between the attacker(s) and defender(s) was formulated as a Stackelberg game problem, and the algorithm to solve the game was given. Based on the equilibrium point of the game, the defender(s) selects specific nodes(s) to place his actuator(s) in order to mitigate the attack effects as far as possible. Two different scenarios, namely single attacker–single defender and multi attackers–multi defenders were considered. The game formulation, its solution, and simulation results were presented for $h$–nearest neighbor platoons with different data transfer structures. The proposed technique can be applied to arbitrary data transfer structures employed in different platoon formation topologies. Besides, the effects of increasing the connectivity among the vehicles on the security level of the platoon have been studied. Some experimental tests were also conducted on a real platoon to demonstrate the applicability of the method in practice. Some open avenues for this research would be to generalize the work to study a platoon consisting of vehicles with different dynamics referred to as "heterogeneous" platoons and to consider the constant time headway spacing policy. Besides, incorporating frequency response analysis in the our proposed method to consider string stability analysis also deserves further research.

## ACKNOWLEDGMENT

The authors would like to thank the Natural Sciences and Engineering Research Council (NSERC) of Canada for their support of this research.

## References

[1] *A Brief History of Car Hacking 2010 to the Present*, 2017. [Online]. Available: https://smart.gi-de.com/2017/08/brief-history-car-hacking-2010-present/.

[2] Y. Abou Harfouch, S. Yuan, and S. Baldi, *An adaptive switched control approach to heterogeneous platooning with intervehicle communication losses*, IEEE Transactions on Control of Network Systems **5** (2017), no. 3, 1434–1444.

[3] S. Amin, G. A. Schwartz, and S. S. Sastry, *Security of interdependent and identical networked control systems*, Automatica **49** (2013), no. 1, 186–192.

[4] M. Amoozadeh et al., *Security vulnerabilities of connected vehicle streams and their impact on cooperative driving*, IEEE Communications Magazine **53** (2015), no. 6, 126–132.

[5] M. Azees, P. Vijayakumar, and L. J. Deborah, *Comprehensive survey on security services in vehicular ad-hoc networks*, IET Intelligent Transport Systems **10** (2016), no. 6, 379–388.

[6] R. H. Bartels and G. W. Stewart, *Solution of the matrix equation $ax + xb = c$*, Communications of the ACM **15** (1972), no. 9, 820–826.

[7] M. H. Basiri, N. L. Azad, and S. Fischmeister, *Attack resilient heterogeneous vehicle platooning using secure distributed nonlinear model predictive control*, *2020 28th Mediterranean Conference on Control and Automation (MED)*, IEEE, 307–312.

[8] M. H. Basiri, N. L. Azad, and S. Fischmeister, *Secure dynamic nonlinear heterogeneous vehicle platooning: Denial-of-service cyber-attack case*, *Security in Cyber-Physical Systems. Studies in Systems, Decision and Control*, vol. 339, Springer Nature, 2021.

[9] M. H. Basiri et al., *Kalman filter based secure state estimation and individual attacked sensor detection in cyber-physical systems*, *2019 American Control Conference (ACC)*, IEEE, 3841–3848.

[10] M. H. Basiri et al., *Security of vehicle platooning: A game-theoretic approach*, IEEE Access **7** (2019), 185565–185579.

[11] M. H. Basiri et al., *Distributed nonlinear model predictive control and metric learning for heterogeneous vehicle platooning with cut-in/cut-out maneuvers*, *2020 59th Conference on Decision and Control (CDC), Jeju Island, Republic of Korea*, IEEE, 2849–2856.

[12] T. Bécsi, S. Aradi, and P. Gáspár, *Security issues and vulnerabilities in connected car systems*, *2015 International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)*, IEEE, 477–482.

[13] Z. A. Biron, S. Dey, and P. Pisu, *Sensor fault diagnosis of connected vehicles under imperfect communication network*, *ASME, Dynamic Systems and Control Conference*, vol. 1, V001T16A003.

[14] Z. A. Biron, S. Dey, and P. Pisu, *Real-time detection and estimation of denial of service attack in connected vehicle systems*, IEEE Transactions on Intelligent Transportation Systems (2018), no. 99, 1–10.

[15] P. N. Brown, H. Borowski, and J. R. Marden, *Security against impersonation attacks in distributed systems*, IEEE Transactions on Control of Network Systems (2018).

[16] D. Caveney, *Cooperative vehicular safety applications*, IEEE Control Systems Magazine **30** (2010), no. 4, 38–53.

[17] D. Chen et al., *Robust stabilization and $H_\infty$ control of cooperative driving system with time delay in variable speed-limited area from cyber-physical perspective*, Asian Journal of Control **22** (2020), no. 1, 373–387.

[18] S. Dadras, R. M. Gerdes, and R. Sharma, *Vehicular platooning in an adversarial environment*, *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, ACM, 167–178.

[19] K. C. Dey et al., *A review of communication, driver characteristics, and controls aspects of cooperative adaptive cruise control (cacc)*, IEEE Transactions on Intelligent Transportation Systems **17** (2016), no. 2, 491–509.

[20] S. M. Dibaji and H. Ishii, *Resilient consensus of second-order agent networks: Asynchronous update rules with delays*, Automatica **81** (2017), 123–132.

[21] Y. Du et al., *A distributed message delivery infrastructure for connected vehicle technology applications*, IEEE Transactions on Intelligent Transportation Systems **19** (2018), no. 3, 787–801.

[22] F. Gao et al., *Distributed adaptive sliding mode control of vehicular platoon with uncertain interaction topology*, IEEE Transactions on Industrial Electronics **65** (2018), no. 8, 6352–6361.

[23] A. Gattami et al., *Establishing safety for heavy duty vehicle platooning: A game theoretical approach*, IFAC Proceedings Volumes **44** (2011), no. 1, 3818–3823.

[24] A. Gupta, C. Langbort, and T. Başar, *Optimal control in the presence of an intelligent jammer with limited actions*, *49th IEEE Conference on Decision and Control (CDC)*, IEEE, 1096–1101.

[25] L. Guvenc et al., *Cooperative adaptive cruise control implementation of team mekar at the grand cooperative driving challenge*, IEEE Transactions on Intelligent Transportation Systems **13** (2012), no. 3, 1062–1074.

[26] S. J. Hammarling, *Numerical solution of the stable, non-negative definite Lyapunov equation lyapunov equation*, IMA Journal of Numerical Analysis **2** (1982), no. 3, 303–323.

[27] H. Hao and P. Barooah, *Stability and robustness of large platoons of vehicles with double-integrator models and nearest neighbor interaction*, International Journal of Robust and Nonlinear Control **23** (2013), no. 18, 2097–2122.

[28] H. Hao, P. Barooah, and J. Veerman, *Effect of network structure on the stability margin of large vehicle formation with distributed control*, *49th IEEE Conference on Decision and Control (CDC)*, IEEE, 4783–4788.

[29] D. He, T. Qiu, and R. Luo, *Fuel efficiency-oriented platooning control of connected nonlinear vehicles: A distributed economic mpc approach*, Asian Journal of Control **22** (2020), no. 4, 1628–1638.

[30] N. Jahanshahi and R. M. Ferrari, *Attack detection and estimation in cooperative vehicles platoons: A sliding mode observer approach*, IFAC-PapersOnLine **51** (2018), no. 23, 212–217.

[31] M. A. Javed and E. B. Hamida, *On the interrelation of security, qos, and safety in cooperative its*, IEEE Transactions on Intelligent Transportation Systems **18** (2017), no. 7, 1943–1957.

[32] D. Jia et al., *A survey on platoon-based vehicular cyber-physical systems*, IEEE communications surveys & tutorials **18** (2016), no. 1, 263–284.

[33] T. Keijzer and R. M. Ferrari, *A sliding mode observer approach for attack detection and estimation in autonomous vehicle platoons using event triggered communication*, *2019 IEEE 58th Conference on Decision and Control (CDC)*, IEEE, 5742–5747.

[34] J.-R. Li and J. White, *Low rank solution of Lyapunov equations*, SIAM Journal on Matrix Analysis and Applications **24** (2002), no. 1, 260–280.

[35] S. E. Li et al., *Dynamical modeling and distributed control of connected and automated vehicles: Challenges and opportunities*, IEEE Intelligent Transportation Systems Magazine **9** (2017), no. 3, 46–58.

[36] Y. Li et al., *Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach*, IEEE Transactions on Automatic Control **60** (2015), no. 10, 2831–2836.

[37] Y. Li et al., *Nonlinear consensus-based connected vehicle platoon control incorporating car-following interactions and heterogeneous time delays*, IEEE Transactions on Intelligent Transportation Systems (2018).

[38] K. Lidström et al., *A modular cacc system integration and design*, IEEE Transactions on Intelligent Transportation Systems **13** (2012), no. 3, 1050.

[39] P. Liu, A. Kurt, and U. Ozguner, *Distributed model predictive control for cooperative and flexible vehicle platooning*, IEEE Transactions on Control Systems Technology (2018), no. 99, 1–14.

[40] M. H. Manshaei et al., *Game theory meets network security and privacy*, ACM Computing Surveys (CSUR) **45** (2013), no. 3, 25.

[41] J. R. Marden, G. Arslan, and J. S. Shamma, *Cooperative control and potential games*, IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics) **39** (2009), no. 6, 1393–1407.

[42] V. Milanés et al., *Cooperative adaptive cruise control in real traffic situations.*, IEEE Trans. Intelligent Transportation Systems **15** (2014), no. 1, 296–305.

[43] C. Nowakowski et al., *Cooperative adaptive cruise control (CACC) for truck platooning: Operational concept alternatives*, 2015.

[44] S. Öncü et al., *Cooperative adaptive cruise control: Network-aware analysis of string stability*, IEEE Transactions on Intelligent Transportation Systems **15** (2014), no. 4, 1527–1537.

[45] F. Pasqualetti, S. Zampieri, and F. Bullo, *Controllability metrics, limitations and algorithms for complex networks*, IEEE Transactions on Control of Network Systems **1** (2014), no. 1, 40–52.

[46] M. Pirani et al., *Graph theoretic approach to the robustness of k-nearest neighbor vehicle platoons*, IEEE Transactions on Intelligent Transportation Systems **18** (2017), no. 11, 3218–3224.

[47] M. Pirani et al., *Resilient estimation and control on k-nearest neighbor platoons: A network-theoretic approach*, IFAC-PapersOnLine **51** (2018), no. 23, 22–27.

[48] J. Ploeg, N. Van De Wouw, and H. Nijmeijer, *Lp string stability of cascaded systems: Application to vehicle platooning*, IEEE Transactions on Control Systems Technology **22** (2013), no. 2, 786–793.

[49] W. B. Qin, M. M. Gomez, and G. Orosz, *Stability analysis of connected cruise control with stochastic delays*, *2014 American Control Conference*, IEEE, 4624–4629.

[50] W. B. Qin and G. Orosz, *Experimental validation of string stability for connected vehicles subject to information delay*, IEEE Transactions on Control Systems Technology (2019).

[51] K. Rabieh, M. M. Mahmoud, and M. Younis, *Privacy-preserving route reporting schemes for traffic management systems*, IEEE Transactions on Vehicular Technology **66** (2017), no. 3, 2703–2713.

[52] M. Raya and J.-P. Hubaux, *Securing vehicular ad hoc networks*, Journal of computer security **15** (2007), no. 1, 39–68.

[53] W. Ren, R. W. Beard, and E. M. Atkins, *Information consensus in multivehicle cooperative control*, IEEE Control systems magazine **27** (2007), no. 2, 71–82.

[54] B. Sakhdari and N. L. Azad, *A distributed reference governor approach to ecological cooperative adaptive cruise control*, IEEE Transactions on Intelligent Transportation Systems **19** (2017), no. 5, 1496–1507.

[55] B. Sakhdari and N. L. Azad, *Adaptive tube-based nonlinear mpc for economic autonomous cruise control of plug-in hybrid electric vehicles*, IEEE Transactions on Vehicular Technology **67** (2018), no. 12, 11390–11401.

[56] E. Semsar-Kazerooni and J. Ploeg, *Performance analysis of a cooperative adaptive cruise controller subject to dynamic time headway*, *16th International IEEE Conference on Intelligent Transportation Systems (ITSC 2013)*, IEEE, 1190–1195.

[57] S. Shafiei, A. M. Kamalirad, and A. Taghavipour, *Robust control of connected vehicles via v2v communication*, Asian Journal of Control **21** (2019), no. 4, 1644–1658.

[58] S. E. Shladover, *Cooperative (rather than autonomous) vehicle-highway automation systems*, IEEE Intelligent Transportation Systems Magazine **1** (2009), no. 1, 10–19.

[59] J. E. Siegel, D. C. Erb, and S. E. Sarma, *A survey of the connected vehicle landscape-architectures, enabling technologies, applications, and development areas*, IEEE Transactions on Intelligent Transportation Systems **19** (2018), no. 8, 2391–2406.

[60] S. S. Stankovic, M. J. Stanojevic, and D. D. Siljak, *Decentralized overlapping control of a platoon of vehicles*, IEEE Transactions on Control Systems Technology **8** (2000), no. 5, 816–832.

[61] T. H. Summers, F. L. Cortesi, and J. Lygeros, *On submodularity and controllability in complex dynamical networks*, IEEE Transactions on Control of Network Systems **3** (2016), no. 1, 91–101.

[62] S. Sundaram and C. N. Hadjicostis, *Distributed function calculation via linear iterative strategies in the presence of malicious agents*, IEEE Transactions on Automatic Control **56** (2010), no. 7, 1495–1508.

[63] D. Swaroop and J. K. Hedrick, *Constant spacing strategies for platooning in automated highway systems*, Journal of dynamic systems, measurement, and control **121** (1999), no. 3, 462–470.

[64] E. Tegling and H. Sandberg, *On the coherence of large-scale networks with distributed pi and pd control*, IEEE control systems letters **1** (2017), no. 1, 170–175.

[65] B. Van Arem, C. J. Van Driel, and R. Visser, *The impact of cooperative adaptive cruise control on traffic-flow characteristics*, IEEE Transactions on Intelligent Transportation Systems **7** (2006), no. 4, 429–436.

[66] Z. Wang and Y.-S. Huang, *Robust decentralized adaptive fuzzy control of large-scale nonaffine nonlinear systems with strong interconnection and application to automated highway systems*, Asian Journal of Control **21** (2019), no. 5, 2387–2394.

[67] S. Woo, H. J. Jo, and D. H. Lee, *A practical wireless attack on the connected car and security protocol for in-vehicle can*, IEEE Transactions on intelligent transportation systems **16** (2015), no. 2, 993–1006.

[68] L. Xiao and F. Gao, *Practical string stability of platoon of adaptive cruise control vehicles*, IEEE Transactions on intelligent transportation systems **12** (2011), no. 4, 1184–1194.

[69] S.-M. Yu et al., *Delayed feedback mpc algorithms of vehicle platoons subject to constraints on measurement range and driving behaviors*, Asian Journal of Control **20** (2018), no. 6, 2260–2270.

[70] T. Zhang, H. Antunes, and S. Aggarwal, *Defending connected vehicles against malware: Challenges and a solution framework*, IEEE Internet of Things journal **1** (2014), no. 1, 10–21.

[71] X. Zhao et al., *An exponential type control design for autonomous vehicle platoon systems*, Asian Journal of Control (2020).

[72] Y. Zheng et al., *Stability and scalability of homogeneous vehicular platoon: Study on the influence of information flow topologies*, IEEE Transactions on Intelligent Transportation Systems **17** (2016), no. 1, 14–26.

[73] Y. Zheng et al., *Stability margin improvement of vehicular platoon considering undirected topology and asymmetric control*, IEEE Transactions on Control Systems Technology **24** (2016), no. 4, 1253–1265.

[74] Q. Zhu and T. Basar, *Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems*, IEEE Control Systems Magazine **35** (2015), no. 1, 46–65.

□